(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10307776 A**

(43) Date of publication of application: **17.11.98**

(51) Int. Cl **G06F 13/00**
G06F 9/06

(21) Application number: **09115634**

(22) Date of filing: **06.05.97**

(71) Applicant: **NEC NIIGATA LTD**

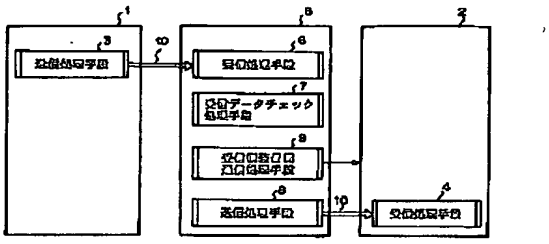
(72) Inventor: **YOKOYAMA MASATOSHI**

(54) **COMPUTER VIRUS RECEPTION MONITOR DEVICE AND ITS SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To automatically prevent a reception-side device from being infected with a computer virus through data communication between computers by making a computer virus check on communication data and informing the reception-side device that a computer virus has been detected in such a case.

SOLUTION: When a transmission-side device 1 sends communication data 10 to the reception-side device 2, the computer virus reception monitor device 5 receives it through a receiving process means 6 before the reception-side device 2 receives the communication data 10. The communication data 10 taken in by the computer virus reception monitor device 5 are checked by a receive data check process means 7 as to a computer virus. If the communication data 10 are infected with a computer virus and illegal, a receive data check process means 7 discards the communication data 10 and informs the reception-side device 2 that the infected illegal data has been sent.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－307776

(43)公開日　平成10年(1998)11月17日

(51)Int.Cl.[6]		識別記号	FI		
G06F	13/00	351	G06F	13/00	351Z
	9/06	550		9/06	550Z

審査請求 有　請求項の数4　OL　（全 5 頁）

(21)出願番号　特願平9－115634

(22)出願日　平成９年(1997) ５月６日

(71)出願人　000190541
新潟日本電気株式会社
新潟県柏崎市大字安田7546番地

(72)発明者　横山　正敏
新潟県柏崎市大字安田7546番地　新潟日本電気株式会社内

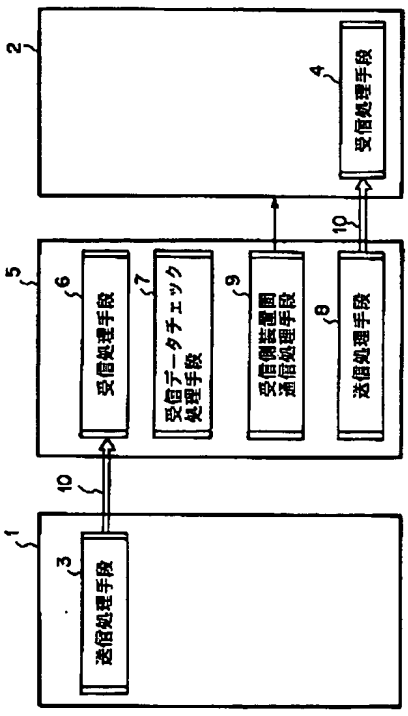
(74)代理人　弁理士　山下　穣平

(54)【発明の名称】　コンピュータウイルス受信監視装置及びそのシステム

(57)【要約】

【課題】　コンピュータ回線網に接続されている受信側装置がコンピュータウイルスに感染した通信データを受信しないようにして、受信側装置のコンピュータウイルスによる感染を未然に防ぐ。

【解決手段】　コンピュータ回線網からデータを受信する受信処理手段と、前記受信処理手段により受信した受信データがコンピュータウイルスに感染しているかどうかを診断する受信データ処理手段と、前記受信データが前記コンピュータウイルスに感染している場合に、これを示す感染信号を受信側装置に知らせる受信側装置間通信処理手段と、前記受信データが前記コンピュータウイルスに感染していない場合に、前記受信データを前記受信側装置に送信する送信処理手段とを備えるコンピュータウイルス受信監視装置をコンピュータ回線網と受信側装置との間に介在させる。



1

【特許請求の範囲】

【請求項１】　コンピュータ回線網と前記コンピュータ回線網を通して送られてくる送信側装置からのデータを受信する受信側装置との間にあり、前記コンピュータ回線網から前記データを受信する受信処理手段と、

前記受信処理手段により受信した受信データがコンピュータウイルスに感染しているかどうかを診断する受信データ処理手段と、

前記受信データが前記コンピュータウイルスに感染している場合に、これを示す感染信号を前記受信側装置に知らせる受信側装置間通信処理手段と、

前記受信データが前記コンピュータウイルスに感染していない場合に、前記受信データを前記受信側装置に送信する送信処理手段とを備えることを特徴とするコンピュータウイルス受信監視装置。

【請求項２】　前記受信データを一時記憶する作業用記憶部と、

前記コンピュータウイルスのパターンを記憶する不正データパターン記憶部と、

制御処理装置とを備え、

前記診断は、前記作業用記憶部に一時記憶されている前記受信データと前記不正データパターン記憶部に記憶されている前記コンピュータウイルスの前記パターンとを前記制御処理装置において比較することによりおこなうことを特徴とする請求項１に記載のコンピュータウイルス受信監視装置。

【請求項３】　請求項１又は２に記載のコンピュータウイルス受信監視装置より前記感染信号を受信したときには受信データを受信しないことを特徴とする受信側装置。

【請求項４】　請求項１又は２に記載のコンピュータウイルス受信監視装置及び請求項３に記載の受信側装置より構成されることを特徴とするコンピュータウイルス受信監視システム。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、コンピュータネットワークにおける送信側装置と受信側装置との間のデータ通信を制御する通信制御装置、及びそれを含むシステムに関するものであり、特に、コンピュータウィルス受信監視装置、及びそれを含むシステムに関するものである。

【０００２】

【従来の技術】図４は特開平６－３１１１４４号公報に掲載の従来の通信制御方法を用いた処理システムの構成を示すブロック図である。図４において、４０１は例えばコンピュータなどの送信側装置、４０２は例えばコンピュータなどの受信側装置、４０３は送信側装置４０１内の送信処理を行う送信処理手段、４０４は受信処理装置４０２内の受信処理を行う受信処理手段、４０５は送

2

信処理手段４０３から受信処理手段４０４へ送信される固定長通信データ、４０６，４０７はチェック用パリティ、４０９は受信データチェック処理手段、４１０は通信初期化処理手段である。

【０００３】次に動作について説明する。固定長通信データ４０５にエラーチェック用パリティ４０６，４０７を設ける。送信処理手段４０３からの固定長通信データ４０５は、受信処理手段４０４で受信され、受信データエラーチェック処理手段４０９でそのデータ４０５のチェック用パリティ４０６，４０７をチェックすることにより正しいか否かが判定される。その固定長通信データ４０５が不正であった場合、通信関係の処理系は通信初期化処理手段４１０で初期化され、これにより通信が復旧される。

【０００４】

【発明が解決しようとする課題】従来の通信制御方法は、受信側装置４０２が固定長通信データの欠除を検出することにより、送信側装置４０１に通信データの再送を要求する、或いは、受信側装置４０２の再初期化を行うことにより通信データの正常性を保証するものであり、通信データが送信側装置４０１や受信側装置４０２にとって本当に無害なものかどうかをこの通信制御方法によってチェックすることができず、コンピュータウイルスに感染された通信データを受信側装置４０２が取り込んでしまう可能性がある。また、受信側装置４０２が受信したデータがコンピュータウイルスに感染しているかどうかを確認する為には、受信データに含まれるデータやプログラムを使用したり実行したりする前に、それらをコンピュータウイルスチェックプログラムによって調べなければならない。

【０００５】［発明の目的］この発明は上記のような問題を解決するためになされたものであり、通信データが受信側装置で受信される前に、通信データに対してコンピュータウイルスチェックをかけて、コンピュータウイルスが検出された場合に、受信側装置にコンピュータウイルスが検出されたことを通知することにより、コンピュータ間のデータ通信による受信側装置のコンピュータウイルス感染を自動的に防止することができるコンピュータウイルス受信監視装置、及びそれを含むシステムを提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明によるコンピュータウイルス受信監視装置は、コンピュータ回線網と前記コンピュータ回線網を通して送られてくる送信側装置からのデータを受信する受信側装置との間にあり、前記コンピュータ回線網から前記データを受信する受信処理手段と、前記受信処理手段により受信した受信データがコンピュータウイルスに感染しているかどうかを診断する受信データ処理手段と、前記受信データが前記コンピュータウイルスに感染している場合に、これを示す感染信

号を前記受信側装置に知らせる受信側装置間通信処理手段と、前記受信データが前記コンピュータウイルスに感染していない場合に、前記受信データを前記受信側装置に送信する送信処理手段とを備えることを特徴とする。

【０００７】また、本発明によるコンピュータウイルス受信監視装置は、前記受信データを一時記憶する作業用記憶部と、前記コンピュータウイルスのパターンを記憶する不正データパターン記憶部と、制御処理装置とを備え、前記診断は、前記作業用記憶部に一時記憶されている前記受信データと前記不正データパターン記憶部に記憶されている前記コンピュータウイルスの前記パターンとを前記制御処理装置において比較することによりおこなうことを特徴とする。

【０００８】更に、本発明による受信側装置は、上記コンピュータウイルス受信監視装置より前記感染信号を受信したときには受信データを受信しないことを特徴とする。

【０００９】更に、本発明によるコンピュータウイルス受信監視システムは、上記コンピュータウイルス受信監視装置及び上記受信側装置より構成されることを特徴とする。

【００１０】［作用］受信側装置が通信データを受信する前にコンピュータウイルス受信監視装置が自動的にコンピュータウイルスチェックを行う。このため、受信側装置は受信データにコンピュータウイルスチェックをかけることなく、受信した直後に受信データに含まれるデータやプログラムを使用できる。また、コンピュータウイルスに感染した通信データは受信側装置に到達する前に破棄されるので、受信側装置はコンピュータウイルスに感染されない。さらに、コンピュータウイルスに感染した通信データがチェック機能により検出され破棄されても、受信データがコンピュータウィルスに感染しているためにデータ破棄したことを受信側装置に通知するので、通信エラーとの区別が容易である。

【００１１】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。本発明の最良の実施の形態は図１を参照すると以下のようになる。コンピュータウイルス受信監視装置５は、送信側装置１と送信側装置１からの通信データ１０を受信する受信側装置２との間にある。コンピュータウイルス受信監視装置５は送信側装置１からの通信データ１０を受信する受信処理手段６をもつ。また、通信データ１０のコンピュータウイルス感染をチェックする受信データチェック処理手段７をもつ。送信処理手段８は受信側装置２に通信データ１０を送信するためのものである。受信側装置間通信処理手段９は、受信した通信データ１０がコンピュータウイルスに感染していることがコンピュータウイルスチェックにより判明した場合に、受信側装置２にコンピュータウイルスに感染している通信データの受信があったことを通知する為のものである。

【００１２】次に図１のブロック図および図２の動作フローチャートを参照してこの実施形態の動作について説明する。送信側装置１が受信側装置２に向けて、通信データ１０を送信すると、受信側装置２が通信データ１０を受信する前に、受信処理手段６によりコンピュータウイルス受信監視装置５がこれを受信する（ステップＳ１）。コンピュータウイルス受信監視装置５に取り込まれた通信データ１０は、受信データチェック処理手段７によりコンピュータウイルスチェックされる（ステップＳ２）。チェックの結果、通信データ１０にコンピュータウイルスの感染が認められなかった場合、コンピュータウイルス受信監視装置５は送信処理手段８により通信データ１０を受信処理手段４を備える受信側装置２へ送る（ステップＳ３）。これにより受信側装置２は通信データ１０をコンピュータウイルスに感染していない通常のデータとして受信する。受信データ１０がコンピュータウイルスに感染している心配がないので、ウイルスチェックをしないでデータにアクセスできる。通信データ１０がコンピュータウイルスに感染していて不正であった場合、コンピュータウイルス受信監視装置５は受信データチェック処理手段７により通信データ１０を破棄し（ステップＳ４）、受信側装置間通信手段９により受信側装置２にコンピュータウイルスに汚染されている不正データが送信されてきたことを通知する（ステップＳ５）。通信データ１０がコンピュータウイルスに汚染されている不正データであった場合は、コンピュータウイルス受信監視装置５より受信側装置２に対して受信側装置間通信処理手段９による通知があるので、単純な通信エラーとの区別は容易である。受信側装置２は、この通知があったときには通信データを受信しない。

【００１３】なお、本実施形態においては、送信側装置１と受信側装置２とをそれぞれ送信専用或いは受信専用として説明したが、送信側装置１と受信側装置２との両方の機能を持つ送受信装置が一般的な形態の装置である。

【００１４】また、本実施形態の受信装置は、パソコン通信などのサーバに使用することもできる。

【００１５】

【実施例】次に、本発明の実施例について図面を参照して詳細に説明する。

【００１６】図３はコンピュータウイルス受信監視装置５及びその周辺の一実施例を示すブロック図である。コンピュータ回線網３０１を通して、図１の送信側装置１から受信側装置２にデータが送信される。制御処理装置３０５は図１における受信処理手段６、受信データチェック処理手段７、送信処理手段８、および受信側装置間通信手段９を制御する為のものでＭＰＵ等により構成されている。制御命令記憶部３０３は制御処理装置３０５の制御命令を記憶する為のもので、コンピュータウイル

5

スの影響を排除する為にＲＯＭ（Read Only Memory）により構成されている。作業用記憶部３０４はコンピュータ回線網３０１より受信した通信データ１０の一時的に記憶する為に使用する為のものでＲＡＭ（Random Access Memory）により構成されている。不正データパターン記憶部３０２は既知のコンピュータウイルスのデータパターンを記憶しておく部分でデータパターンの追加を考慮して、ＰＲＯＭ（Programmable Read Only Memory）により構成されている。不正データパターン記憶部３０２は図１の受信データチェック処理手段７として使用される。また、作業用記憶部３０４は図１の受信処理手段６、送信処理手段８、受信側装置間通信手段９を使用する際にも利用する。

【００１７】次に図３のブロック図および図２の動作フローチャートを参照して本実施例の動作について説明する。送信側装置１がコンピュータ回線網３０１を通して受信側装置２に向けて、通信データ１０を送信すると、受信側装置２が通信データ１０を受信する前に制御命令記憶部３０３に記憶されているデータ受信を行う命令を制御処理装置３０５が実行する。その実行の度にコンピュータウイルス受信監視装置５は通信データ１０を作業用記憶部３０４に記憶する（ステップＳ１）。制御処理装置３０５が制御命令記憶部３０３に記憶されている命令により不正データパターン記憶部３０２の不正データパターンと作業用記憶部３０４に記憶された通信データ１０を比較する（ステップＳ２）。比較の結果、不正データパターンと共通のデータパターンが通信データ１０に認められない場合には、コンピュータウイルスの感染はないものとして、制御処理装置３０５は制御命令記憶部３０３に記憶されている受信側装置２への通信データ１０の受け渡し命令を実行し、通信データ１０を送信する（ステップＳ３）。不正データパターンと共通のデータパターンが通信データ１０が認められた場合には、通信データ１０がコンピュータウイルスに感染しているとして通信データ１０を破棄し（ステップＳ４）、制御処理装置３０５は制御命令記憶部３０３に記憶されている本体システム２への通知命令を実行し、受信側装置２に不正データが送信されてきたことを通知する（ステップＳ５）。

【００１８】

【発明の効果】以上説明したように本発明によれば、送信側装置から受信側装置に通信データが送信された場

6

合、受信側装置に通信データが届く前にコンピュータウイルス受信監視装置がそのデータを受信し、コンピュータウイルスチェックを行い、コンピュータウイルスに感染されていない通信データのみを受信側装置に送信する為、受信側装置のデータ通信によるコンピュータウイルス感染を未然に防げる。また、コンピュータウイルスチェックをデータ受信時に自動的に行っていることで受信側装置がデータ受信後に改めてチェックする必要がなくなる。

【図面の簡単な説明】

【図１】本発明によるコンピュータウイルス受信監視装置、及びそれを含むデータ送受信システムの構成を示す第１のブロック図である。

【図２】本発明によるコンピュータウイルス受信監視装置の制御処理を示すフローチャートである。

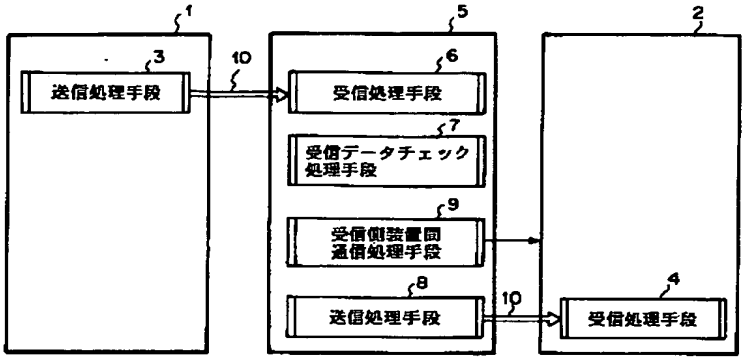
【図３】本発明によるコンピュータウイルス受信監視装置、及びそれを含むデータ送受信システムの構成を示す第２のブロック図である。

【図４】従来の通信制御方法を用いたデータ送受信システムの構成を示すブロック図である。

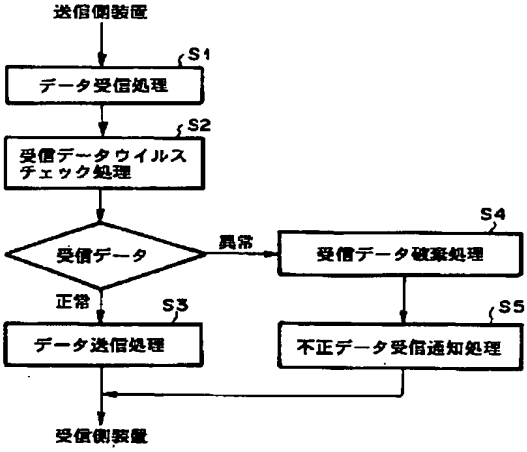
【符号の説明】

１　送信側装置
２　受信側装置
３　送信処理手段
４　受信処理手段
５　コンピュータウイルス受信監視装置
６　受信処理手段
７　受信データチェック処理手段
８　送信処理手段
９　受信側装置間通信処理手段
１０　通信データ
３０１　コンピュータ回線網
３０２　不正データパターン記憶部
３０３　制御命令記憶部
３０４　作業用記憶部
３０５　制御処理装置
Ｓ１　データ受信処理
Ｓ２　受信データチェック処理
Ｓ３　データ送信処理
Ｓ４　受信データ破棄処理
Ｓ５　不正データ受信通知処理

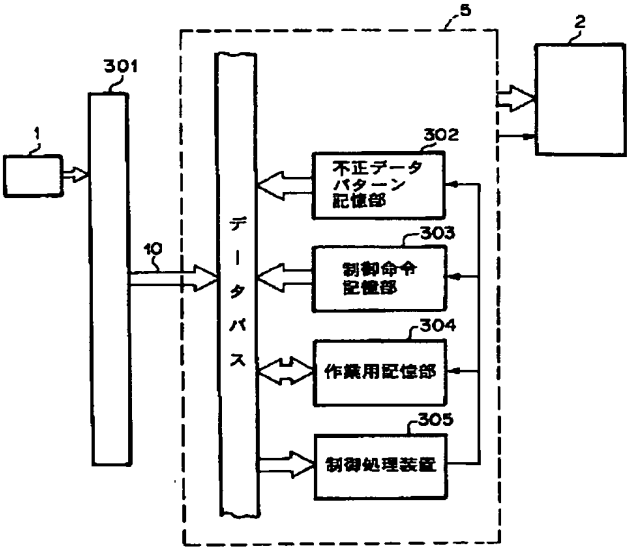
【図１】


1
5
2
3
10
送信処理手段
受信処理手段
6
7
受信データチェック処理手段
9
受信側装置間通信処理手段
8
送信処理手段
10
4
受信処理手段

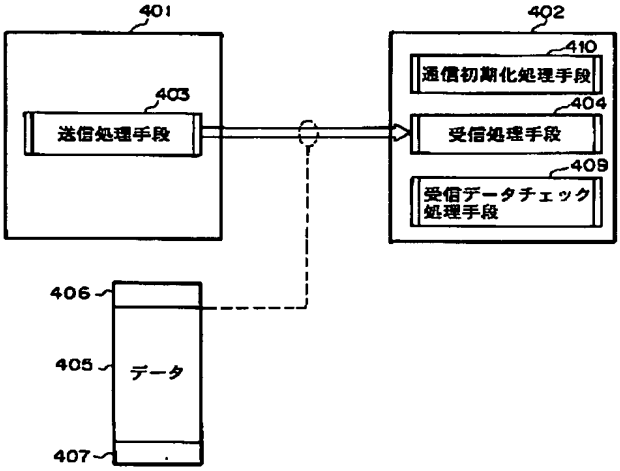
【図２】


送信側装置
S1
データ受信処理
S2
受信データウイルスチェック処理
受信データ
異常
S4
受信データ破棄処理
正常
S3
データ送信処理
S5
不正データ受信通知処理
受信側装置

【図３】


5
2
301
1
10
データバス
302
不正データパターン記憶部
303
制御命令記憶部
304
作業用記憶部
305
制御処理装置

【図４】


401
402
403
送信処理手段
410
通信初期化処理手段
404
受信処理手段
409
受信データチェック処理手段
406
405
データ
407

[0011]

[Embodiments] Next, an embodiment of the present invention will be described with reference to the drawings. The most preferable embodiment of the present invention will be described with reference to Fig. 1. Namely, a computer virus reception monitoring device 5 is interposed between a transmitting-side device 1 and a receiving-side device 2 that receives communication data 10 from the transmitting-side device 1. The computer virus reception monitoring device 5 includes a receiving means 6 that receives the communication data 10 sent from the transmitting-side device 1. Moreover, the computer virus reception monitoring device 5 includes a received data checking means 7 that checks if the communication data 10 is infected with a computer virus. The transmitting means 8 transmits the communication data 10 to the receiving-side device 2. If the computer virus check reveals that the received communication data 10 has been infected with a computer virus, a communicating-with-receiving-side device means 9 notifies the receiving-side device 2 that communication data infected with a computer virus has been received.

[0012] Next, the actions to be performed according to the present embodiment will be described with reference to the block diagram of Fig. 1 and the flowchart of Fig. 2. When the transmitting-side device 1 transmits communication data 10 to the receiving-side device 2, and before the receiving-side device 2 receives the communication data 10, the receiving means 6 included in the computer virus reception monitoring device 5 receives the communication data 10 (step S1). The received data checking means 7 checks if the communication data 10 fetched into the computer virus reception monitoring device 5 is infected with a computer virus (step S2). If the result of the check demonstrates that infection of the communication data 10 with a computer virus is not recognized, the transmitting means 8 included in the computer virus reception monitoring device 5 transmits

the communication data 10 to the receiving-side device 2 that includes the receiving means 4 (step S3). Consequently, the receiving-side device 2 receives the communication data 10 as normal data uninfected with a computer virus. As the receiving-side device 2 need not care about whether the received data 10 is infected with a computer virus, the receiving-side device 2 can access the data without performing a virus check. If the communication data 10 is infected with a computer virus and is regarded as illegal data, the received data checking means included in the computer virus reception monitoring device 5 discards the communication data 10 (step S4). The communicating-with-receiving-side device means 9 notifies the receiving-side device 2 that illegal data contaminated with a computer virus has arrived (step S5). If the communication data 10 is illegal data contaminated with a computer virus, the communicating-with-receiving-side device means 9 included in the computer virus reception monitoring device 5 notifies the receiving-side device of the fact. A simple communication error can therefore be readily discriminated. When the receiving-side device 2 receives the notification, the receiving-side device 2 receives no communication data.

[0013] According to the present embodiment, the transmitting-side device 1 and receiving-side device 2 are dedicated to transmission or reception. Transmitter-receivers having the capabilities of both the transmitting-side device 1 and receiving-side device 2 are generally adopted as the devices.

[0014] Moreover, the receiving-side device employed in the present embodiment may be adopted as a server on a network on which personal computers communicate with one another.

[0015]

[Examples] Next, an example of the present invention will be described with reference to the drawings.

[0016] Fig. 3 is a block diagram showing an example of the computer virus reception monitoring device 5 and its peripherals. The transmitting-side device 1 shown in Fig. 1

transmits data to the receiving-side device 2 shown therein over a computer network 301. A control unit 305 is formed with an MPU or the like in order to control each of the receiving means 6, received data checking means 7, transmitting means 8, and communicating-with-receiving-side device means 9. A control instruction sent from the control unit 305 is stored in a control instruction memory 303. The control instruction memory 303 is formed with a read-only memory (ROM) in an effort to remove the adverse effect of a computer virus. A working memory 304 is used to temporarily store communication data 10 received from the computer network 301, and formed with a random access memory (RAM). Data patterns of known computer viruses are stored in an illegal data pattern memory 302 that is formed with a programmable read-only memory (PROM) in consideration of the possibility that other data pattern may be added. The illegal data pattern memory 302 is used as the received data checking means 7 shown in Fig. 1. Moreover, the working memory 304 is utilized at the time of using the receiving means 6, transmitting means 8, and communicating-with-receiving-side device means 9.

[0017] Next, actions to be performed in the present example will be described with reference to the block diagram of Fig. 3 and the flowchart of Fig. 2. The transmitting-side device 1 transmits communication data 10 to the receiving-side device 2 over the computer network 301. Before the receiving-side device 2 receives the communication data 10, the control unit 305 executes a data reception instruction that is stored in the control instruction memory 303. Every time the instruction is executed, the computer virus reception monitoring device 5 stores the communication data 10 in the working memory 304 (step S1). In response to a instruction stored in the control instruction memory 303, the control unit 305 compares the communication data 10 stored in the working memory 304 with the illegal data patterns stored in the illegal data pattern memory 303 (step S2). If the result of the comparison demonstrates that no data pattern

identical to any of the illegal data patterns is detected in the communication data 10, the control unit 305 judges that the communication data 10 is not infected with a computer virus. The control unit 305 then executes an instruction that the communication data 10 should be handed to the receiving-side device 2 which is stored in the control instruction memory 303, and transmits the communication data 10 accordingly (step S3). If a data pattern identical to any of the illegal data patterns is detected in the communication data 10, it is judged that the communication data 10 has been infected with a computer virus. The communication data 10 is therefore discarded (step S4). The control unit 305 executes an instruction that the main system 2 should be notified which is stored in the control instruction memory 303. The control unit notifies the receiving-side device 2 that illegal data has arrived (step S5).

[0018]

[Advantages] As described above, according to the present invention, when communication data is transmitted from a transmitting-side device to a receiving-side device, before the communication data reaches the receiving-side device, a computer virus reception monitoring device receives the data and checks the data for a computer virus. Only communication data uninfected with a computer virus is transmitted to the receiving-side device. Consequently, the receiving-side device can be prevented from being infected with a computer virus through data communication. Moreover, as the computer virus check is automatically performed at the time of data reception, the receiving-side device need not check for a computer virus after receiving the data.